

.70 If not already performed during the overall review stage of the audit, the auditor should perform analytical procedures relating to revenue, as discussed in paragraph .29, through the end of the reporting period.

.71 Determining which particular trends and relationships may indicate a risk of material misstatement due to fraud requires professional judgment. Unusual relationships involving year-end revenue and income often are particularly relevant. These might include, for example, (a) uncharacteristically large amounts of income being reported in the last week or two of the reporting period from unusual transactions, as well as (b) income that is inconsistent with trends in cash flow from operations.

.72 Some unusual or unexpected analytical relationships may have been identified and may indicate a risk of material misstatement due to fraud because management or employees generally are unable to manipulate certain information to create seemingly normal or expected relationships. Some examples are as follows:

- The relationship of net income to cash flows from operations may appear unusual because management recorded fictitious revenues and receivables but was unable to manipulate cash.
- Changes in inventory, accounts payable, sales, or cost of sales from the prior period to the current period may be inconsistent, indicating a possible employee theft of inventory, because the employee was unable to manipulate all of the related accounts.
- A comparison of the entity's profitability to industry trends, which management cannot manipulate, may indicate trends or differences for further consideration when identifying risks of material misstatement due to fraud.
- A comparison of bad debt write-offs to comparable industry data, which employees cannot manipulate, may provide unexplained relationships that could indicate a possible theft of cash receipts.
- An unexpected or unexplained relationship between sales volume as determined from the accounting records and production statistics maintained by operations personnel—which may be more difficult for management to manipulate—may indicate a possible misstatement of sales.

.73 The auditor also should consider whether responses to inquiries throughout the audit about analytical relationships have been vague or implausible, or have produced evidence that is inconsistent with other audit evidence accumulated during the audit. [Revised, March 2006, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 105.]

***.74 Evaluating the risks of material misstatement due to fraud at or near the date of the auditor's report.*** At or near the completion of fieldwork, the auditor should evaluate whether the accumulated results of auditing procedures and other observations (for example, conditions and analytical relationships noted in paragraphs .69 through .73) affect the assessment of the risks of material misstatement due to fraud made earlier in the audit. This evaluation primarily is a qualitative matter based on the auditor's judgment. Such an evaluation may provide further insight about the risks of material misstatement due to fraud and whether there is a need to perform additional or different audit procedures. As part of this evaluation, the auditor with final responsibility for the audit should ascertain that there has been appropriate

communication with the other audit team members throughout the audit regarding information or conditions indicative of risks of material misstatement due to fraud.<sup>30</sup>

**.75 Responding to misstatements that may be the result of fraud.** When audit test results identify misstatements in the financial statements, the auditor should consider whether such misstatements may be indicative of fraud.<sup>31</sup> That determination affects the auditor's evaluation of materiality and the related responses necessary as a result of that evaluation.<sup>32</sup>

**.76** If the auditor believes that misstatements are or may be the result of fraud, but the effect of the misstatements is not material to the financial statements, the auditor nevertheless should evaluate the implications, especially those dealing with the organizational position of the person(s) involved. For example, fraud involving misappropriations of cash from a small petty cash fund normally would be of little significance to the auditor in assessing the risk of material misstatement due to fraud because both the manner of operating the fund and its size would tend to establish a limit on the amount of potential loss, and the custodianship of such funds normally is entrusted to a nonmanagement employee.<sup>33</sup> Conversely, if the matter involves higher-level management, even though the amount itself is not material to the financial statements, it may be indicative of a more pervasive problem, for example, implications about the integrity of management.<sup>34</sup> In such circumstances, the auditor should reevaluate the assessment of the risk of material misstatement due to fraud and its resulting impact on (a) the nature, timing, and extent of the tests of balances or transactions and (b) the assessment of the effectiveness of controls if control risk was assessed below the maximum.

**.77** If the auditor believes that the misstatement is or may be the result of fraud, and either has determined that the effect could be material to the financial statements or has been unable to evaluate whether the effect is material, the auditor should:

- a. Attempt to obtain additional audit evidence to determine whether material fraud has occurred or is likely to have occurred, and, if so, its effect on the financial statements and the auditor's report thereon.<sup>35</sup>

---

<sup>30</sup> To accomplish this communication, the auditor with final responsibility for the audit may want to arrange another discussion among audit team members about the risks of material misstatement due to fraud (see paragraphs .14 through .18). [Footnote renumbered by the issuance of Statement on Auditing Standards No. 113, November 2006.]

<sup>31</sup> See footnote 4. [Footnote renumbered by the issuance of Statement on Auditing Standards No. 113, November 2006.]

<sup>32</sup> Section 312.60 states in part, "Qualitative considerations also influence the auditor in reaching a conclusion as to whether misstatements are material." Section 312.59 states, "As a result of the interaction of quantitative and qualitative considerations in materiality judgments, misstatements of relatively small amounts that come to the auditor's attention could have a material effect on the financial statements." [Footnote revised, March 2006, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 107. Footnote renumbered by the issuance of Statement on Auditing Standards No. 113, November 2006.]

<sup>33</sup> However, see paragraphs .79 through .82 of this section for a discussion of the auditor's communication responsibilities. [Footnote renumbered by the issuance of Statement on Auditing Standards No. 113, November 2006.]

<sup>34</sup> Section 312.10 states that there is a distinction between the auditor's response to detected misstatements due to error and those due to fraud. When fraud is detected, the auditor should consider the implications for the integrity of management or employees and the possible effect on other aspects of the audit. [Footnote revised, March 2006, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 107. Footnote renumbered by the issuance of Statement on Auditing Standards No. 113, November 2006.]

<sup>35</sup> See section 508 for guidance on auditors' reports issued in connection with audits of financial statements. [Footnote renumbered by the issuance of Statement on Auditing Standards No. 113, November 2006.]

- b. Consider the implications for other aspects of the audit (see paragraph .76).
- c. Discuss the matter and the approach for further investigation with an appropriate level of management that is at least one level above those involved, and with senior management and those charged with governance.<sup>36</sup>
- d. If appropriate, suggest that the client consult with legal counsel.

[Revised, March 2006, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 105. Revised, April 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 114.]

.78 The auditor's consideration of the risks of material misstatement and the results of audit tests may indicate such a significant risk of material misstatement due to fraud that the auditor should consider withdrawing from the engagement and communicating the reasons for withdrawal to those charged with governance.<sup>[37]</sup> Whether the auditor concludes that withdrawal from the engagement is appropriate may depend on (a) the implications about the integrity of management and (b) the diligence and cooperation of management or the board of directors in investigating the circumstances and taking appropriate action. Because of the variety of circumstances that may arise, it is not possible to definitively describe when withdrawal is appropriate.<sup>38</sup> The auditor may wish to consult with legal counsel when considering withdrawal from an engagement. [Revised, April 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 114.]

## Communicating About Possible Fraud to Management, Those Charged With Governance, and Others<sup>39</sup>

.79 Whenever the auditor has determined that there is evidence that fraud may exist, that matter should be brought to the attention of an appropriate level of management. This is appropriate even if the matter might be considered inconsequential, such as a minor defalcation by an employee at a low level in the entity's organization. Fraud involving senior management and fraud (whether caused by senior management or other employees) that causes

---

<sup>36</sup> If the auditor believes senior management may be involved, discussion of the matter directly with those charged with governance may be appropriate. [Footnote renumbered by the issuance of Statement on Auditing Standards No. 113, November 2006. Footnote revised, April 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 114.]

<sup>[37]</sup> [Footnote renumbered by the issuance of Statement on Auditing Standards No. 113, November 2006. Footnote deleted due to conforming changes necessary due to the issuance of Statement on Auditing Standards No. 114.]

<sup>38</sup> If the auditor, subsequent to the date of the report on the audited financial statements, becomes aware that facts existed at that date that might have affected the report had the auditor been aware of such facts, the auditor should refer to section 561, *Subsequent Discovery of Facts Existing at the Date of the Auditor's Report*, for guidance. Furthermore, section 315, *Communications Between Predecessor and Successor Auditors*, paragraphs .21 and .22, provide guidance regarding communication with a predecessor auditor. [Footnote renumbered by the issuance of Statement on Auditing Standards No. 113, November 2006.]

<sup>39</sup> The requirements to communicate noted in paragraphs .79 through .82 extend to any intentional misstatement of financial statements (see paragraph .03). However, the communication may use terms other than fraud—for example, irregularity, intentional misstatement, misappropriation, or defalcations—if there is possible confusion with a legal definition of fraud or other reason to prefer alternative terms. [Footnote renumbered by the issuance of Statement on Auditing Standards No. 113, November 2006.]

a material misstatement of the financial statements should be reported directly to those charged with governance. In addition, the auditor should reach an understanding with those charged with governance regarding the nature and extent of communications with them about misappropriations perpetrated by lower-level employees. [Revised, April 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 114.]

.80 If the auditor, as a result of the assessment of the risks of material misstatement, has identified risks of material misstatement due to fraud that have continuing control implications (whether or not transactions or adjustments that could be the result of fraud have been detected), the auditor should consider whether these risks represent significant deficiencies or material weaknesses in the entity's internal control that should be communicated to management and those charged with governance.<sup>[40]</sup> (See section 325, *Communicating Internal Control Related Matters Identified in an Audit*, paragraph .04). The auditor also should consider whether the absence of or deficiencies in programs and controls to mitigate specific risks of fraud or to otherwise help prevent, deter, and detect fraud (see paragraph .44) represent significant deficiencies or material weaknesses that should be communicated to management and those charged with governance. [Revised, May 2006, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 112.]

.81 The auditor also may wish to communicate other risks of fraud identified as a result of the assessment of the risks of material misstatements due to fraud. Such a communication may be a part of an overall communication with those charged with governance of business and financial statement risks affecting the entity and/or in conjunction with the auditor communication about the quality of the entity's accounting principles (see section 380.11). [Revised, April 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 114.]

.82 The disclosure of possible fraud to parties other than the client's senior management and those charged with governance ordinarily is not part of the auditor's responsibility and ordinarily would be precluded by the auditor's ethical or legal obligations of confidentiality unless the matter is reflected in the auditor's report. The auditor should recognize, however, that in the following circumstances a duty to disclose to parties outside the entity may exist:

- a. To comply with certain legal and regulatory requirements<sup>41</sup>
- b. To a successor auditor when the successor makes inquiries in accordance with section 315, *Communications Between Predecessor and Successor Auditors*<sup>42</sup>
- c. In response to a subpoena

<sup>[40]</sup> [Footnote deleted to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 112. Footnote renumbered by the issuance of Statement on Auditing Standards No. 113, November 2006.]

<sup>41</sup> These requirements include reports in connection with the termination of the engagement, such as when the entity reports an auditor change on Form 8-K and the fraud or related risk factors constitute a *reportable event* or is the source of a *disagreement*, as these terms are defined in Item 304 of Regulation S-K. These requirements also include reports that may be required, under certain circumstances, pursuant to Section 10A(b)1 of the Securities Exchange Act of 1934 relating to an illegal act that has a material effect on the financial statements. [Footnote renumbered by the issuance of Statement on Auditing Standards No. 113, November 2006.]

<sup>42</sup> Section 315 requires the specific permission of the client. [Footnote renumbered by the issuance of Statement on Auditing Standards No. 113, November 2006.]



- d. To a funding agency or other specified agency in accordance with requirements for the audits of entities that receive governmental financial assistance<sup>43</sup>

Because potential conflicts between the auditor's ethical and legal obligations for confidentiality of client matters may be complex, the auditor may wish to consult with legal counsel before discussing matters covered by paragraphs .79 through .81 with parties outside the client. [Revised, April 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 114.]

## Documenting the Auditor's Consideration of Fraud

.83 The auditor should document the following:

- The discussion among engagement personnel in planning the audit regarding the susceptibility of the entity's financial statements to material misstatement due to fraud, including how and when the discussion occurred, the audit team members who participated, and the subject matter discussed (See paragraphs .14 through .17.)
- The procedures performed to obtain information necessary to identify and assess the risks of material misstatement due to fraud (See paragraphs .19 through .34.)
- Specific risks of material misstatement due to fraud that were identified (see paragraphs .35 through .45), and a description of the auditor's response to those risks (See paragraphs .46 through .56.)
- If the auditor has not identified in a particular circumstance, improper revenue recognition as a risk of material misstatement due to fraud, the reasons supporting the auditor's conclusion (See paragraph .41.)
- The results of the procedures performed to further address the risk of management override of controls (See paragraphs .58 through .67.)
- Other conditions and analytical relationships that caused the auditor to believe that additional auditing procedures or other responses were required and any further responses the auditor concluded were appropriate, to address such risks or other conditions (See paragraphs .68 through .73.)
- The nature of the communications about fraud made to management, those charged with governance, and others (See paragraphs .79 through .82.)

[Revised, April 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 114.]

## Effective Date

.84 This section is effective for audits of financial statements for periods beginning on or after December 15, 2002. Early application of the provisions of this section is permissible.

---

<sup>43</sup> For example, *Government Auditing Standards* (the Yellow Book) require auditors to report fraud or illegal acts directly to parties outside the audited entity in certain circumstances. [Footnote renumbered by the issuance of Statement on Auditing Standards No. 113, November 2006.]

.85

## Appendix

### Examples of Fraud Risk Factors

A.1 This appendix contains examples of risk factors discussed in paragraphs .31 through .33 of the section. Separately presented are examples relating to the two types of fraud relevant to the auditor's consideration—that is, fraudulent financial reporting and misappropriation of assets. For each of these types of fraud, the risk factors are further classified based on the three conditions generally present when material misstatements due to fraud occur: (a) incentives/pressures, (b) opportunities, and (c) attitudes/rationalizations. Although the risk factors cover a broad range of situations, they are only examples and, accordingly, the auditor may wish to consider additional or different risk factors. Not all of these examples are relevant in all circumstances, and some may be of greater or lesser significance in entities of different size or with different ownership characteristics or circumstances. Also, the order of the examples of risk factors provided is not intended to reflect their relative importance or frequency of occurrence.

### Risk Factors Relating to Misstatements Arising From Fraudulent Financial Reporting

A.2 The following are examples of risk factors relating to misstatements arising from fraudulent financial reporting.

#### Incentives/Pressures

- a. Financial stability or profitability is threatened by economic, industry, or entity operating conditions, such as (or as indicated by):
  - High degree of competition or market saturation, accompanied by declining margins
  - High vulnerability to rapid changes, such as changes in technology, product obsolescence, or interest rates
  - Significant declines in customer demand and increasing business failures in either the industry or overall economy
  - Operating losses making the threat of bankruptcy, foreclosure, or hostile takeover imminent
  - Recurring negative cash flows from operations and an inability to generate cash flows from operations while reporting earnings and earnings growth
  - Rapid growth or unusual profitability, especially compared to that of other companies in the same industry
  - New accounting, statutory, or regulatory requirements
- b. Excessive pressure exists for management to meet the requirements or expectations of third parties due to the following:
  - Profitability or trend level expectations of investment analysts, institutional investors, significant creditors, or other external parties (particularly expectations that are unduly aggressive or unrealistic), including expectations created by management in, for example, overly optimistic press releases or annual report messages

## The Standards of Field Work

- Need to obtain additional debt or equity financing to stay competitive—including financing of major research and development or capital expenditures
  - Marginal ability to meet exchange listing requirements or debt repayment or other debt covenant requirements
  - Perceived or real adverse effects of reporting poor financial results on significant pending transactions, such as business combinations or contract awards
- c. Information available indicates that management's or those charged with governance's personal financial situation is threatened by the entity's financial performance arising from the following:
- Significant financial interests in the entity
  - Significant portions of their compensation (for example, bonuses, stock options, and earn-out arrangements) being contingent upon achieving aggressive targets for stock price, operating results, financial position, or cash flow<sup>1</sup>
  - Personal guarantees of debts of the entity
- d. There is excessive pressure on management or operating personnel to meet financial targets set up by those charged with governance or management, including sales or profitability incentive goals.

## Opportunities

- a. The nature of the industry or the entity's operations provides opportunities to engage in fraudulent financial reporting that can arise from the following:
- Significant related-party transactions not in the ordinary course of business or with related entities not audited or audited by another firm
  - A strong financial presence or ability to dominate a certain industry sector that allows the entity to dictate terms or conditions to suppliers or customers that may result in inappropriate or non-arm's-length transactions
  - Assets, liabilities, revenues, or expenses based on significant estimates that involve subjective judgments or uncertainties that are difficult to corroborate
  - Significant, unusual, or highly complex transactions, especially those close to period end that pose difficult "substance over form" questions
  - Significant operations located or conducted across international borders in jurisdictions where differing business environments and cultures exist
  - Significant bank accounts or subsidiary or branch operations in tax-haven jurisdictions for which there appears to be no clear business justification

---

<sup>1</sup> Management incentive plans may be contingent upon achieving targets relating only to certain accounts or selected activities of the entity, even though the related accounts or activities may not be material to the entity as a whole.

## Consideration of Fraud in a Financial Statement Audit

199

- b. There is ineffective monitoring of management as a result of the following:
  - Domination of management by a single person or small group (in a nonowner-managed business) without compensating controls
  - Ineffective oversight over the financial reporting process and internal control by those charged with governance
- c. There is a complex or unstable organizational structure, as evidenced by the following:
  - Difficulty in determining the organization or individuals that have controlling interest in the entity
  - Overly complex organizational structure involving unusual legal entities or managerial lines of authority
  - High turnover of senior management, counsel, or board members
- d. Internal control components are deficient as a result of the following:
  - Inadequate monitoring of controls, including automated controls and controls over interim financial reporting (where external reporting is required)
  - High turnover rates or employment of ineffective accounting, internal audit, or information technology staff
  - Ineffective accounting and information systems, including situations involving significant deficiencies or material weaknesses in internal control

**Attitudes/Rationalizations**

Risk factors reflective of attitudes/rationalizations by those charged with governance, management, or employees, that allow them to engage in and/or justify fraudulent financial reporting, may not be susceptible to observation by the auditor. Nevertheless, the auditor who becomes aware of the existence of such information should consider it in identifying the risks of material misstatement arising from fraudulent financial reporting. For example, auditors may become aware of the following information that may indicate a risk factor:

- Ineffective communication, implementation, support, or enforcement of the entity's values or ethical standards by management or the communication of inappropriate values or ethical standards
- Nonfinancial management's excessive participation in or preoccupation with the selection of accounting principles or the determination of significant estimates
- Known history of violations of securities laws or other laws and regulations, or claims against the entity, its senior management, or board members alleging fraud or violations of laws and regulations
- Excessive interest by management in maintaining or increasing the entity's stock price or earnings trend
- A practice by management of committing to analysts, creditors, and other third parties to achieve aggressive or unrealistic forecasts
- Management failing to correct known significant deficiencies or material weaknesses in internal control on a timely basis
- An interest by management in employing inappropriate means to minimize reported earnings for tax-motivated reasons



- Recurring attempts by management to justify marginal or inappropriate accounting on the basis of materiality
- The relationship between management and the current or predecessor auditor is strained, as exhibited by the following:
  - Frequent disputes with the current or predecessor auditor on accounting, auditing, or reporting matters
  - Unreasonable demands on the auditor, such as unreasonable time constraints regarding the completion of the audit or the issuance of the auditor's report
  - Formal or informal restrictions on the auditor that inappropriately limit access to people or information or the ability to communicate effectively with those charged with governance
  - Domineering management behavior in dealing with the auditor, especially involving attempts to influence the scope of the auditor's work or the selection or continuance of personnel assigned to or consulted on the audit engagement

### **Risk Factors Relating to Misstatements Arising From Misappropriation of Assets**

A.3 Risk factors that relate to misstatements arising from misappropriation of assets are also classified according to the three conditions generally present when fraud exists: incentives/pressures, opportunities, and attitudes/rationalizations. Some of the risk factors related to misstatements arising from fraudulent financial reporting also may be present when misstatements arising from misappropriation of assets occur. For example, ineffective monitoring of management and weaknesses in internal control may be present when misstatements due to either fraudulent financial reporting or misappropriation of assets exist. The following are examples of risk factors related to misstatements arising from misappropriation of assets.

#### **Incentives/Pressures**

- a. Personal financial obligations may create pressure on management or employees with access to cash or other assets susceptible to theft to misappropriate those assets.
- b. Adverse relationships between the entity and employees with access to cash or other assets susceptible to theft may motivate those employees to misappropriate those assets. For example, adverse relationships may be created by the following:
  - Known or anticipated future employee layoffs
  - Recent or anticipated changes to employee compensation or benefit plans
  - Promotions, compensation, or other rewards inconsistent with expectations

#### **Opportunities**

- a. Certain characteristics or circumstances may increase the susceptibility of assets to misappropriation. For example, opportunities to misappropriate assets increase when there are the following:
  - Large amounts of cash on hand or processed
  - Inventory items that are small in size, of high value, or in high demand

## Consideration of Fraud in a Financial Statement Audit

201

- Easily convertible assets, such as bearer bonds, diamonds, or computer chips
  - Fixed assets that are small in size, marketable, or lacking observable identification of ownership
- b. Inadequate internal control over assets may increase the susceptibility of misappropriation of those assets. For example, misappropriation of assets may occur because there is the following:
- Inadequate segregation of duties or independent checks
  - Inadequate management oversight of employees responsible for assets, for example, inadequate supervision or monitoring of remote locations
  - Inadequate job applicant screening of employees with access to assets
  - Inadequate recordkeeping with respect to assets
  - Inadequate system of authorization and approval of transactions (for example, in purchasing)
  - Inadequate physical safeguards over cash, investments, inventory, or fixed assets
  - Lack of complete and timely reconciliations of assets
  - Lack of timely and appropriate documentation of transactions, for example, credits for merchandise returns
  - Lack of mandatory vacations for employees performing key control functions
  - Inadequate management understanding of information technology, which enables information technology employees to perpetrate a misappropriation
  - Inadequate access controls over automated records, including controls over and review of computer systems event logs.

**Attitudes/Rationalizations**

Risk factors reflective of employee attitudes/rationalizations that allow them to justify misappropriations of assets, are generally not susceptible to observation by the auditor. Nevertheless, the auditor who becomes aware of the existence of such information should consider it in identifying the risks of material misstatement arising from misappropriation of assets. For example, auditors may become aware of the following attitudes or behavior of employees who have access to assets susceptible to misappropriation:

- Disregard for the need for monitoring or reducing risks related to misappropriations of assets
- Disregard for internal control over misappropriation of assets by overriding existing controls or by failing to correct known internal control deficiencies
- Behavior indicating displeasure or dissatisfaction with the company or its treatment of the employee
- Changes in behavior or lifestyle that may indicate assets have been misappropriated

[Revised, May 2006, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 112; Revised, April 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 114.]

## Exhibit

### Management Antifraud Programs and Controls

#### Guidance to Help Prevent, Deter, and Detect Fraud

(This exhibit is reprinted for the reader's convenience but is not an integral part of the section.)

This document is being issued jointly by the following organizations:

American Institute of Certified Public Accountants

Association of Certified Fraud Examiners

Financial Executives International

Information Systems Audit and Control Association

The Institute of Internal Auditors

Institute of Management Accountants

Society for Human Resource Management

In addition, we would also like to acknowledge the American Accounting Association, the Defense Industry Initiative, and the National Association of Corporate Directors for their review of the document and helpful comments and materials.

We gratefully acknowledge the valuable contribution provided by the Anti-Fraud Detection Subgroup:

Daniel D. Montgomery, *Chair*

Toby J.F. Bishop

Dennis H. Chookaszian

Susan A. Finn

Dana Hermanson

David L. Landsittel

Carol A. Langelier

Joseph T. Wells

Janice Wilkins

Finally, we thank the staff of the American Institute of Certified Public Accountants for their support on this project:

Charles E. Landes

*Director*

*Audit and Attest Standards*

Richard Lanza

*Senior Program Manager*

*Chief Operating Office*

Kim M. Gibson

*Senior Technical Manager*

*Audit and Attest Standards*

Hugh Kelsey

*Program Manager*

*Knowledge Management*

This document was commissioned by the Fraud Task Force of the AICPA's Auditing Standards Board. This document has not been adopted, approved, disapproved, or otherwise acted upon by a board, committee, governing body, or membership of the above issuing organizations.

## Preface

Some organizations have significantly lower levels of misappropriation of assets and are less susceptible to fraudulent financial reporting than other organizations because these organizations take proactive steps to prevent or deter fraud. It is only those organizations that seriously consider fraud risks and take proactive steps to create the right kind of climate to reduce its occurrence that have success in preventing fraud. This document identifies the key participants in this antifraud effort, including the board of directors, management, internal and independent auditors, and certified fraud examiners.

Management may develop and implement some of these programs and controls in response to specific identified risks of material misstatement of financial statements due to fraud. In other cases, these programs and controls may be a part of the entity's enterprise-wide risk management activities.

Management is responsible for designing and implementing systems and procedures for the prevention and detection of fraud and, along with the board of directors, for ensuring a culture and environment that promotes honesty and ethical behavior. However, because of the characteristics of fraud, a material misstatement of financial statements due to fraud may occur notwithstanding the presence of programs and controls such as those described in this document.



## Introduction

Fraud can range from minor employee theft and unproductive behavior to misappropriation of assets and fraudulent financial reporting. Material financial statement fraud can have a significant adverse effect on an entity's market value, reputation, and ability to achieve its strategic objectives. A number of highly publicized cases have heightened the awareness of the effects of fraudulent financial reporting and have led many organizations to be more proactive in taking steps to prevent or deter its occurrence. Misappropriation of assets, though often not material to the financial statements, can nonetheless result in substantial losses to an entity if a dishonest employee has the incentive and opportunity to commit fraud.

The risk of fraud can be reduced through a combination of prevention, deterrence, and detection measures. However, fraud can be difficult to detect because it often involves concealment through falsification of documents or collusion among management, employees, or third parties. Therefore, it is important to place a strong emphasis on fraud prevention, which may reduce opportunities for fraud to take place, and fraud deterrence, which could persuade individuals that they should not commit fraud because of the likelihood of detection and punishment. Moreover, prevention and deterrence measures are much less costly than the time and expense required for fraud detection and investigation.

An entity's management has both the responsibility and the means to implement measures to reduce the incidence of fraud. The measures an organization takes to prevent and deter fraud also can help create a positive workplace environment that can enhance the entity's ability to recruit and retain high-quality employees.

Research suggests that the most effective way to implement measures to reduce wrongdoing is to base them on a set of core values that are embraced by the entity. These values provide an overarching message about the key principles guiding all employees' actions. This provides a platform upon which a more detailed code of conduct can be constructed, giving more specific guidance about permitted and prohibited behavior, based on applicable laws and the organization's values. Management needs to clearly articulate that all employees will be held accountable to act within the organization's code of conduct.

This document identifies measures entities can implement to prevent, deter, and detect fraud. It discusses these measures in the context of three fundamental elements. Broadly stated, these fundamental elements are (1) create and maintain a *culture* of honesty and high ethics; (2) *evaluate* the risks of fraud and implement the processes, procedures, and controls needed to mitigate the risks and reduce the opportunities for fraud; and (3) develop an appropriate *oversight* process. Although the entire management team shares the responsibility for implementing and monitoring these activities, with oversight from the board of directors, the entity's chief executive officer (CEO) should initiate and support such measures. Without the CEO's active support, these measures are less likely to be effective.

The information presented in this document generally is applicable to entities of all sizes. However, the degree to which certain programs and controls are applied in smaller, less-complex entities and the formality of their application are likely to differ from larger organizations. For example, management of a smaller entity (or the owner of an owner-managed entity), along with those charged with governance of the financial reporting process, are responsible for creating a culture of honesty and high ethics. Management also is responsible for implementing a system of internal controls commensurate with the nature and size of the organization, but smaller entities may find that certain types

of control activities are not relevant because of the involvement of and controls applied by management. However, all entities must make it clear that unethical or dishonest behavior will not be tolerated.

## Creating a Culture of Honesty and High Ethics

It is the organization's responsibility to create a culture of honesty and high ethics and to clearly communicate acceptable behavior and expectations of each employee. Such a culture is rooted in a strong set of core values (or value system) that provides the foundation for employees as to how the organization conducts its business. It also allows an entity to develop an ethical framework that covers (1) fraudulent financial reporting, (2) misappropriation of assets, and (3) corruption as well as other issues.<sup>1</sup>

Creating a culture of honesty and high ethics should include the following.

### *Setting the Tone at the Top*

Directors and officers of corporations set the "tone at the top" for ethical behavior within any organization. Research in moral development strongly suggests that honesty can best be reinforced when a proper example is set—sometimes referred to as the tone at the top. The management of an entity cannot act one way and expect others in the entity to behave differently.

In many cases, particularly in larger organizations, it is necessary for management to both behave ethically and openly communicate its expectations for ethical behavior because most employees are not in a position to observe management's actions. Management must show employees through its words and actions that dishonest or unethical behavior will not be tolerated, even if the result of the action benefits the entity. Moreover, it should be evident that all employees will be treated equally, regardless of their position.

For example, statements by management regarding the absolute need to meet operating and financial targets can create undue pressures that may lead employees to commit fraud to achieve them. Setting unachievable goals for employees can give them two unattractive choices: fail or cheat. In contrast, a statement from management that says, "We are aggressive in pursuing our targets, while requiring truthful financial reporting at all times," clearly indicates to employees that integrity is a requirement. This message also conveys that the entity has "zero tolerance" for unethical behavior, including fraudulent financial reporting.

The cornerstone of an effective antifraud environment is a culture with a strong value system founded on integrity. This value system often is reflected in a code of conduct.<sup>2</sup> The code of conduct should reflect the core values of the entity and guide employees in making appropriate decisions during their workday. The code of conduct might include such topics as ethics, confidentiality, conflicts of interest, intellectual property, sexual harassment, and fraud.<sup>3</sup> For a code of

<sup>1</sup> Corruption includes bribery and other illegal acts.

<sup>2</sup> An entity's value system also could be reflected in an ethics policy, a statement of business principles, or some other concise summary of guiding principles.

<sup>3</sup> Although the discussion in this document focuses on fraud, the subject of fraud often is considered in the context of a broader set of principles that govern an organization. Some organizations, however, may elect to develop a fraud policy separate from an ethics policy. Specific examples of topics in a fraud policy might include a requirement to comply with all laws and regulations and explicit guidance regarding making payments to obtain contracts, holding pricing discussions with competitors, environmental discharges, relationships with vendors, and maintenance of accurate books and records.

conduct to be effective, it should be communicated to all personnel in an understandable fashion. It also should be developed in a participatory and positive manner that will result in both management and employees taking ownership of its content. Finally, the code of conduct should be included in an employee handbook or policy manual, or in some other formal document or location (for example, the entity's intranet) so it can be referred to when needed.

Senior financial officers hold an important and elevated role in corporate governance. While members of the management team, they are uniquely capable and empowered to ensure that all stakeholders' interests are appropriately balanced, protected, and preserved. For examples of codes of conduct, see Attachment 1, "AICPA 'CPA's Handbook of Fraud and Commercial Crime Prevention,' An Organizational Code of Conduct," and Attachment 2, "Financial Executives International Code of Ethics Statement" provided by Financial Executives International. In addition, visit the Institute of Management Accountant's Ethics Center at [www.imanet.org](http://www.imanet.org) for their members' standards of ethical conduct.

### ***Creating a Positive Workplace Environment***

Research results indicate that wrongdoing occurs less frequently when employees have positive feelings about an entity than when they feel abused, threatened, or ignored. Without a positive workplace environment, there are more opportunities for poor employee morale, which can affect an employee's attitude about committing fraud against an entity. Factors that detract from a positive work environment and may increase the risk of fraud include:

- Top management that does not seem to care about or reward appropriate behavior
- Negative feedback and lack of recognition for job performance
- Perceived inequities in the organization
- Autocratic rather than participative management
- Low organizational loyalty or feelings of ownership
- Unreasonable budget expectations or other financial targets
- Fear of delivering "bad news" to supervisors and/or management
- Less-than-competitive compensation
- Poor training and promotion opportunities
- Lack of clear organizational responsibilities
- Poor communication practices or methods within the organization

The entity's human resources department often is instrumental in helping to build a corporate culture and a positive work environment. Human resource professionals are responsible for implementing specific programs and initiatives, consistent with management's strategies, that can help to mitigate many of the detractors mentioned above. Mitigating factors that help create a positive work environment and reduce the risk of fraud may include:

- Recognition and reward systems that are in tandem with goals and results
- Equal employment opportunities
- Team-oriented, collaborative decision-making policies
- Professionally administered compensation programs
- Professionally administered training programs and an organizational priority of career development

Employees should be empowered to help create a positive workplace environment and support the entity's values and code of conduct. They should be given the opportunity to provide input to the development and updating of the entity's code of conduct, to ensure that it is relevant, clear, and fair. Involving employees in this fashion also may effectively contribute to the oversight of the entity's code of conduct and an environment of ethical behavior (see the section titled "Developing an Appropriate Oversight Process").

Employees should be given the means to obtain advice internally before making decisions that appear to have significant legal or ethical implications. They should also be encouraged and given the means to communicate concerns, anonymously if preferred, about potential violations of the entity's code of conduct, without fear of retribution. Many organizations have implemented a process for employees to report on a confidential basis any actual or suspected wrongdoing, or potential violations of the code of conduct or ethics policy. For example, some organizations use a telephone "hotline" that is directed to or monitored by an ethics officer, fraud officer, general counsel, internal audit director, or another trusted individual responsible for investigating and reporting incidents of fraud or illegal acts.

### ***Hiring and Promoting Appropriate Employees***

Each employee has a unique set of values and personal code of ethics. When faced with sufficient pressure and a perceived opportunity, some employees will behave dishonestly rather than face the negative consequences of honest behavior. The threshold at which dishonest behavior starts, however, will vary among individuals. If an entity is to be successful in preventing fraud, it must have effective policies that minimize the chance of hiring or promoting individuals with low levels of honesty, especially for positions of trust.

Proactive hiring and promotion procedures may include:

- Conducting background investigations on individuals being considered for employment or for promotion to a position of trust<sup>4</sup>
- Thoroughly checking a candidate's education, employment history, and personal references
- Periodic training of all employees about the entity's values and code of conduct, (training is addressed in the following section)
- Incorporating into regular performance reviews an evaluation of how each individual has contributed to creating an appropriate workplace environment in line with the entity's values and code of conduct
- Continuous objective evaluation of compliance with the entity's values and code of conduct, with violations being addressed immediately

### ***Training***

New employees should be trained at the time of hiring about the entity's values and its code of conduct. This training should explicitly cover expectations of all employees regarding (1) their duty to communicate certain matters; (2) a list of the types of matters, including actual or suspected fraud, to be communicated along with specific examples; and (3) information on how to communicate those matters. There also should be an affirmation from senior management regarding employee expectations and communication responsibilities. Such training should include an element of "fraud awareness," the tone of which should be

---

<sup>4</sup> Some organizations also have considered follow-up investigations, particularly for employees in positions of trust, on a periodic basis (for example, every five years) or as circumstances dictate.



positive but nonetheless stress that fraud can be costly (and detrimental in other ways) to the entity and its employees.

In addition to training at the time of hiring, employees should receive refresher training periodically thereafter. Some organizations may consider ongoing training for certain positions, such as purchasing agents or employees with financial reporting responsibilities. Training should be specific to an employee's level within the organization, geographic location, and assigned responsibilities. For example, training for senior manager level personnel would normally be different from that of nonsupervisory employees, and training for purchasing agents would be different from that of sales representatives.

### **Confirmation**

Management needs to clearly articulate that all employees will be held accountable to act within the entity's code of conduct. All employees within senior management and the finance function, as well as other employees in areas that might be exposed to unethical behavior (for example, procurement, sales and marketing) should be required to sign a code of conduct statement annually, at a minimum.

Requiring periodic confirmation by employees of their responsibilities will not only reinforce the policy but may also deter individuals from committing fraud and other violations and might identify problems before they become significant. Such confirmation may include statements that the individual understands the entity's expectations, has complied with the code of conduct, and is not aware of any violations of the code of conduct other than those the individual lists in his or her response. Although people with low integrity may not hesitate to sign a false confirmation, most people will want to avoid making a false statement in writing. Honest individuals are more likely to return their confirmations and to disclose what they know (including any conflicts of interest or other personal exceptions to the code of conduct). Thorough follow-up by internal auditors or others regarding nonreplies may uncover significant issues.

### **Discipline**

The way an entity reacts to incidents of alleged or suspected fraud will send a strong deterrent message throughout the entity, helping to reduce the number of future occurrences. The following actions should be taken in response to an alleged incident of fraud:

- A thorough investigation of the incident should be conducted.<sup>5</sup>
- Appropriate and consistent actions should be taken against violators.
- Relevant controls should be assessed and improved.
- Communication and training should occur to reinforce the entity's values, code of conduct, and expectations.

Expectations about the consequences of committing fraud must be clearly communicated throughout the entity. For example, a strong statement from management that dishonest actions will not be tolerated, and that violators may be terminated and referred to the appropriate authorities, clearly establishes consequences and can be a valuable deterrent to wrongdoing. If wrongdoing occurs

---

<sup>5</sup> Many entities of sufficient size are employing antifraud professionals, such as certified fraud examiners, who are responsible for resolving allegations of fraud within the organization and who also assist in the detection and deterrence of fraud. These individuals typically report their findings internally to the corporate security, legal, or internal audit departments. In other instances, such individuals may be empowered directly by the board of directors or its audit committee.

and an employee is disciplined, it can be helpful to communicate that fact, on a no-name basis, in an employee newsletter or other regular communication to employees. Seeing that other people have been disciplined for wrongdoing can be an effective deterrent, increasing the perceived likelihood of violators being caught and punished. It also can demonstrate that the entity is committed to an environment of high ethical standards and integrity.

## Evaluating Antifraud Processes and Controls

Neither fraudulent financial reporting nor misappropriation of assets can occur without a perceived opportunity to commit and conceal the act. Organizations should be proactive in reducing fraud opportunities by (1) identifying and measuring fraud risks, (2) taking steps to mitigate identified risks, and (3) implementing and monitoring appropriate preventive and detective internal controls and other deterrent measures.

### *Identifying and Measuring Fraud Risks*

Management has primary responsibility for establishing and monitoring all aspects of the entity's fraud risk-assessment and prevention activities.<sup>6</sup> Fraud risks often are considered as part of an enterprise-wide risk management program, though they may be addressed separately.<sup>7</sup> The fraud risk-assessment process should consider the vulnerability of the entity to fraudulent activity (fraudulent financial reporting, misappropriation of assets, and corruption) and whether any of those exposures could result in a material misstatement of the financial statements or material loss to the organization. In identifying fraud risks, organizations should consider organizational, industry, and country-specific characteristics that influence the risk of fraud.

The nature and extent of management's risk assessment activities should be commensurate with the size of the entity and complexity of its operations. For example, the risk assessment process is likely to be less formal and less structured in smaller entities. However, management should recognize that fraud can occur in organizations of any size or type, and that almost any employee may be capable of committing fraud given the right set of circumstances. Accordingly, management should develop a heightened "fraud awareness" and an appropriate fraud risk-management program, with oversight from those charged with governance.

### *Mitigating Fraud Risks*

It may be possible to reduce or eliminate certain fraud risks by making changes to the entity's activities and processes. An entity may choose to sell certain segments of its operations, cease doing business in certain locations, or reorganize its business processes to eliminate unacceptable risks. For example, the risk of misappropriation of funds may be reduced by implementing a central lockbox at a bank to receive payments instead of receiving money at the entity's various locations. The risk of corruption may be reduced by closely monitoring the

---

<sup>6</sup> Management may elect to have internal audit play an active role in the development, monitoring, and ongoing assessment of the entity's fraud risk-management program. This may include an active role in the development and communication of the entity's code of conduct or ethics policy, as well as in investigating actual or alleged instances of noncompliance.

<sup>7</sup> Some organizations may perform a periodic self-assessment using questionnaires or other techniques to identify and measure risks. Self-assessment may be less reliable in identifying the risk of fraud due to a lack of experience with fraud (although many organizations experience some form of fraud and abuse, material financial statement fraud or misappropriation of assets is a rare event for most) and because management may be unwilling to acknowledge openly that they might commit fraud given sufficient pressure and opportunity.

entity's procurement process. The risk of financial statement fraud may be reduced by implementing shared services centers to provide accounting services to multiple segments, affiliates, or geographic locations of an entity's operations. A shared services center may be less vulnerable to influence by local operations managers and may be able to implement more extensive fraud detection measures cost-effectively.

### ***Implementing and Monitoring Appropriate Internal Controls***

Some risks are inherent in the environment of the entity, but most can be addressed with an appropriate system of internal control. Once fraud risk assessment has taken place, the entity can identify the processes, controls, and other procedures that are needed to mitigate the identified risks. Effective internal control will include a well-developed control environment, an effective and secure information system, and appropriate control and monitoring activities.<sup>8</sup> Because of the importance of information technology in supporting operations and the processing of transactions, management also needs to implement and maintain appropriate controls, whether automated or manual, over computer-generated information.

In particular, management should evaluate whether appropriate internal controls have been implemented in any areas management has identified as posing a higher risk of fraudulent activity, as well as controls over the entity's financial reporting process. Because fraudulent financial reporting may begin in an interim period, management also should evaluate the appropriateness of internal controls over interim financial reporting.

Fraudulent financial reporting by upper-level management typically involves override of internal controls within the financial reporting process. Because management has the ability to override controls, or to influence others to perpetrate or conceal fraud, the need for a strong value system and a culture of ethical financial reporting becomes increasingly important. This helps create an environment in which other employees will decline to participate in committing a fraud and will use established communication procedures to report any requests to commit wrongdoing. The potential for management override also increases the need for appropriate oversight measures by those charged with governance, as discussed in the following section.

Fraudulent financial reporting by lower levels of management and employees may be deterred or detected by appropriate monitoring controls, such as having higher-level managers review and evaluate the financial results reported by individual operating units or subsidiaries. Unusual fluctuations in results of particular reporting units, or the lack of expected fluctuations, may indicate potential manipulation by departmental or operating unit managers or staff.

### **Developing an Appropriate Oversight Process**

To effectively prevent or deter fraud, an entity should have an appropriate oversight function in place. Oversight can take many forms and can be performed by many within and outside the entity, under the overall oversight of the audit committee (or those charged with governance, such as the board of directors, where no audit committee exists).

---

<sup>8</sup> The report of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission, *Internal Control—Integrated Framework*, provides reasonable criteria for management to use in evaluating the effectiveness of the entity's system of internal control.

***Audit Committee or Those Charged With Governance***

The audit committee (or those charged with governance where no audit committee exists) should evaluate management's identification of fraud risks, implementation of antifraud measures, and creation of the appropriate "tone at the top." Active oversight by the audit committee can help to reinforce management's commitment to creating a culture with "zero tolerance" for fraud. An entity's audit committee also should ensure that senior management (in particular, the CEO) implements appropriate fraud deterrence and prevention measures to better protect investors, employees, and other stakeholders. The audit committee's evaluation and oversight not only helps make sure that senior management fulfills its responsibility, but also can serve as a deterrent to senior management engaging in fraudulent activity (that is, by ensuring an environment is created whereby any attempt by senior management to involve employees in committing or concealing fraud would lead promptly to reports from such employees to appropriate persons, including the audit committee).

The audit committee also plays an important role in helping those charged with governance fulfill their oversight responsibilities with respect to the entity's financial reporting process and the system of internal control.<sup>9</sup> In exercising this oversight responsibility, the audit committee should consider the potential for management override of controls or other inappropriate influence over the financial reporting process. For example, the audit committee may obtain from the internal auditors and independent auditors their views on management's involvement in the financial reporting process and, in particular, the ability of management to override information processed by the entity's financial reporting system (for example, the ability for management or others to initiate or record nonstandard journal entries). The audit committee also may consider reviewing the entity's reported information for reasonableness compared with prior or forecasted results, as well as with peers or industry averages. In addition, information received in communications from the independent auditors<sup>10</sup> can assist the audit committee in assessing the strength of the entity's internal control and the potential for fraudulent financial reporting.

As part of its oversight responsibilities, the audit committee should encourage management to provide a mechanism for employees to report concerns about unethical behavior, actual or suspected fraud, or violations of the entity's code of conduct or ethics policy. The committee should then receive periodic reports describing the nature, status, and eventual disposition of any fraud or unethical conduct. A summary of the activity, follow-up and disposition also should be provided to all of those charged with governance.

If senior management is involved in fraud, the next layer of management may be the most likely to be aware of it. As a result, the audit committee (and others of those charged with governance) should consider establishing an open line of communication with members of management one or two levels below senior management to assist in identifying fraud at the highest levels of the

---

<sup>9</sup> See the Report of the NACD Blue Ribbon Commission on the Audit Committee, (Washington, D.C.: National Association of Corporate Directors, 2000). For the board's role in the oversight of risk management, see Report of the NACD Blue Ribbon Commission on Risk Oversight, (Washington, D.C.: National Association of Corporate Directors, 2002).

<sup>10</sup> See section 325, *Communicating Internal Control Related Matters Identified in an Audit*, and section 380, *The Auditor's Communication With Those Charged With Governance*. [Footnote revised, May 2006, due to conforming changes necessary due to the issuance of Statement on Standards No. 112. Footnote revised, April 2007, due to conforming changes necessary due to the issuance of Statement on Standards No. 114.]



organization or investigating any fraudulent activity that might occur.<sup>11</sup> The audit committee typically has the ability and authority to investigate any alleged or suspected wrongdoing brought to its attention. Most audit committee charters empower the committee to investigate any matters within the scope of its responsibilities, and to retain legal, accounting, and other professional advisers as needed to advise the committee and assist in its investigation.

All audit committee members should be financially literate, and each committee should have at least one financial expert. The financial expert should possess:

- An understanding of generally accepted accounting principles and audits of financial statements prepared under those principles. Such understanding may have been obtained either through education or experience. It is important for someone on the audit committee to have a working knowledge of those principles and standards.
- Experience in the preparation and/or the auditing of financial statements of an entity of similar size, scope and complexity as the entity on whose board the committee member serves. The experience would generally be as a chief financial officer, chief accounting officer, controller, or auditor of a similar entity. This background will provide a necessary understanding of the transactional and operational environment that produces the issuer's financial statements. It will also bring an understanding of what is involved in, for example, appropriate accounting estimates, accruals, and reserve provisions, and an appreciation of what is necessary to maintain a good internal control environment.
- Experience in internal governance and procedures of audit committees, obtained either as an audit committee member, a senior corporate manager responsible for answering to the audit committee, or an external auditor responsible for reporting on the execution and results of annual audits.

### **Management**

Management is responsible for overseeing the activities carried out by employees, and typically does so by implementing and monitoring processes and controls such as those discussed previously. However, management also may initiate, participate in, or direct the commission and concealment of a fraudulent act. Accordingly, the audit committee (or those charged with governance where no audit committee exists) has the responsibility to oversee the activities of senior management and to consider the risk of fraudulent financial reporting involving the override of internal controls or collusion (see discussion on the audit committee and board of directors above).

Public companies should include a statement in the annual report acknowledging management's responsibility for the preparation of the financial statements and for establishing and maintaining an effective system of internal control. This will help improve the public's understanding of the respective roles of management and the auditor. This statement has also been generally referred to as a "Management Report" or "Management Certificate." Such a statement can provide a convenient vehicle for management to describe the nature and manner of preparation of the financial information and the adequacy of the

---

<sup>11</sup> *Report of the NACD Best Practices Council: Coping with Fraud and Other Illegal Activity, A Guide for Directors, CEOs, and Senior Managers* (1998) sets forth "basic principles" and "implementation approaches" for dealing with fraud and other illegal activity.

internal accounting controls. Logically, the statement should be presented in close proximity to the formal financial statements. For example, it could appear near the independent auditor's report, or in the financial review or management analysis section.

### ***Internal Auditors***

An effective internal audit team can be extremely helpful in performing aspects of the oversight function. Their knowledge about the entity may enable them to identify indicators that suggest fraud has been committed. The *Standards for the Professional Practice of Internal Auditing* (IIA Standards), issued by the Institute of Internal Auditors, state, "The internal auditor should have sufficient knowledge to identify the indicators of fraud but is not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud." Internal auditors also have the opportunity to evaluate fraud risks and controls and to recommend action to mitigate risks and improve controls. Specifically, the IIA Standards require internal auditors to assess risks facing their organizations. This risk assessment is to serve as the basis from which audit plans are devised and against which internal controls are tested. The IIA Standards require the audit plan to be presented to and approved by the audit committee (or board of directors where no audit committee exists). The work completed as a result of the audit plan provides assurance on which management's assertion about controls can be made.

Internal audits can be both a detection and a deterrence measure. Internal auditors can assist in the deterrence of fraud by examining and evaluating the adequacy and the effectiveness of the system of internal control, commensurate with the extent of the potential exposure or risk in the various segments of the organization's operations. In carrying out this responsibility, internal auditors should, for example, determine whether:

- The organizational environment fosters control consciousness.
- Realistic organizational goals and objectives are set.
- Written policies (for example, a code of conduct) exist that describe prohibited activities and the action required whenever violations are discovered.
- Appropriate authorization policies for transactions are established and maintained.
- Policies, practices, procedures, reports, and other mechanisms are developed to monitor activities and safeguard assets, particularly in high-risk areas.
- Communication channels provide management with adequate and reliable information.
- Recommendations need to be made for the establishment or enhancement of cost-effective controls to help deter fraud.

Internal auditors may conduct proactive auditing to search for corruption, misappropriation of assets, and financial statement fraud. This may include the use of computer-assisted audit techniques to detect particular types of fraud. Internal auditors also can employ analytical and other procedures to isolate anomalies and perform detailed reviews of high-risk accounts and transactions to identify potential financial statement fraud. The internal auditors should have an independent reporting line directly to the audit committee, to enable them to express any concerns about management's commitment to appropriate internal controls or to report suspicions or allegations of fraud involving senior management.

***Independent Auditors***

Independent auditors can assist management and the board of directors (or audit committee) by providing an assessment of the entity's process for identifying, assessing, and responding to the risks of fraud. Those charged with governance, such as the board of directors or audit committee, should have an open and candid dialogue with the independent auditors regarding management's risk assessment process and the system of internal control. Such a dialogue should include a discussion of the susceptibility of the entity to fraudulent financial reporting and the entity's exposure to misappropriation of assets.

***Certified Fraud Examiners***

Certified fraud examiners may assist the audit committee and board of directors with aspects of the oversight process either directly or as part of a team of internal auditors or independent auditors. Certified fraud examiners can provide extensive knowledge and experience about fraud that may not be available within a corporation. They can provide more objective input into management's evaluation of the risk of fraud (especially fraud involving senior management, such as financial statement fraud) and the development of appropriate antifraud controls that are less vulnerable to management override. They can assist the audit committee and board of directors in evaluating the fraud risk assessment and fraud prevention measures implemented by management. Certified fraud examiners also conduct examinations to resolve allegations or suspicions of fraud, reporting either to an appropriate level of management or to the audit committee or board of directors, depending upon the nature of the issue and the level of personnel involved.

***Other Information***

To obtain more information on fraud and implementing antifraud programs and controls, please go to the following Web sites where additional materials, guidance, and tools can be found.

American Institute of Certified Public Accountants	<a href="http://www.aicpa.org">www.aicpa.org</a>
Association of Certified Fraud Examiners	<a href="http://www.cfenet.com">www.cfenet.com</a>
Financial Executives International	<a href="http://www.fei.org">www.fei.org</a>
Information Systems Audit and Control Association	<a href="http://www.isaca.org">www.isaca.org</a>
The Institute of Internal Auditors	<a href="http://www.theiia.org">www.theiia.org</a>
Institute of Management Accountants	<a href="http://www.imanet.org">www.imanet.org</a>
National Association of Corporate Directors	<a href="http://www.nacdonline.org">www.nacdonline.org</a>
Society for Human Resource Management	<a href="http://www.shrm.org">www.shrm.org</a>

## Attachment 1: AICPA "CPA's Handbook of Fraud and Commercial Crime Prevention," An Organizational Code of Conduct

The following is an example of an organizational code of conduct, which includes definitions of what is considered unacceptable, and the consequences of any breaches thereof. The specific content and areas addressed in an entity's code of conduct should be specific to that entity.

### *Organizational Code of Conduct*

The Organization and its employees must, at all times, comply with all applicable laws and regulations. The Organization will not condone the activities of employees who achieve results through violation of the law or unethical business dealings. This includes any payments for illegal acts, indirect contributions, rebates, and bribery. The Organization does not permit any activity that fails to stand the closest possible public scrutiny.

All business conduct should be well above the minimum standards required by law. Accordingly, employees must ensure that their actions cannot be interpreted as being, in any way, in contravention of the laws and regulations governing the Organization's worldwide operations.

Employees uncertain about the application or interpretation of any legal requirements should refer the matter to their superior; who, if necessary, should seek the advice of the legal department.

### *General Employee Conduct*

The Organization expects its employees to conduct themselves in a businesslike manner. Drinking, gambling, fighting, swearing, and similar unprofessional activities are strictly prohibited while on the job.

Employees must not engage in sexual harassment, or conduct themselves in a way that could be construed as such, for example, by using inappropriate language, keeping or posting inappropriate materials in their work area, or accessing inappropriate materials on their computer.

### *Conflicts of Interest*

The Organization expects that employees will perform their duties conscientiously, honestly, and in accordance with the best interests of the Organization. Employees must not use their position or the knowledge gained as a result of their position for private or personal advantage. Regardless of the circumstances, if employees sense that a course of action they have pursued, are presently pursuing, or are contemplating pursuing may involve them in a conflict of interest with their employer, they should immediately communicate all the facts to their superior.

### *Outside Activities, Employment, and Directorships*

All employees share a serious responsibility for the Organization's good public relations, especially at the community level. Their readiness to help with religious, charitable, educational, and civic activities brings credit to the Organization and is encouraged. Employees must, however, avoid acquiring any business interest or participating in any other activity outside the Organization that would, or would appear to:

- Create an excessive demand upon their time and attention, thus depriving the Organization of their best efforts on the job.
- Create a conflict of interest—an obligation, interest, or distraction—that may interfere with the independent exercise of judgment in the Organization's best interest.



*Relationships With Clients and Suppliers*

Employees should avoid investing in or acquiring a financial interest for their own accounts in any business organization that has a contractual relationship with the Organization, or that provides goods or services, or both to the Organization, if such investment or interest could influence or create the impression of influencing their decisions in the performance of their duties on behalf of the Organization.

*Gifts, Entertainment, and Favors*

Employees must not accept entertainment, gifts, or personal favors that could, in any way, influence, or appear to influence, business decisions in favor of any person or organization with whom or with which the Organization has, or is likely to have, business dealings. Similarly, employees must not accept any other preferential treatment under these circumstances because their position with the Organization might be inclined to, or be perceived to, place them under obligation.

*Kickbacks and Secret Commissions*

Regarding the Organization's business activities, employees may not receive payment or compensation of any kind, except as authorized under the Organization's remuneration policies. In particular, the Organization strictly prohibits the acceptance of kickbacks and secret commissions from suppliers or others. Any breach of this rule will result in immediate termination and prosecution to the fullest extent of the law.

*Organization Funds and Other Assets*

Employees who have access to Organization funds in any form must follow the prescribed procedures for recording, handling, and protecting money as detailed in the Organization's instructional manuals or other explanatory materials, or both. The Organization imposes strict standards to prevent fraud and dishonesty. If employees become aware of any evidence of fraud and dishonesty, they should immediately advise their superior or the Law Department so that the Organization can promptly investigate further.

When an employee's position requires spending Organization funds or incurring any reimbursable personal expenses, that individual must use good judgment on the Organization's behalf to ensure that good value is received for every expenditure.

Organization funds and all other assets of the Organization are for Organization purposes only and not for personal benefit. This includes the personal use of organizational assets, such as computers.

*Organization Records and Communications*

Accurate and reliable records of many kinds are necessary to meet the Organization's legal and financial obligations and to manage the affairs of the Organization. The Organization's books and records must reflect in an accurate and timely manner all business transactions. The employees responsible for accounting and recordkeeping must fully disclose and record all assets, liabilities, or both, and must exercise diligence in enforcing these requirements.

Employees must not make or engage in any false record or communication of any kind, whether internal or external, including but not limited to:

- False expense, attendance, production, financial, or similar reports and statements
- False advertising, deceptive marketing practices, or other misleading representations

*Dealing With Outside People and Organizations*

Employees must take care to separate their personal roles from their Organization positions when communicating on matters not involving Organization business. Employees must not use organization identification, stationery, supplies, and equipment for personal or political matters.

When communicating publicly on matters that involve Organization business, employees must not presume to speak for the Organization on any topic, unless they are certain that the views they express are those of the Organization, and it is the Organization's desire that such views be publicly disseminated.

When dealing with anyone outside the Organization, including public officials, employees must take care not to compromise the integrity or damage the reputation of either the Organization, or any outside individual, business, or government body.

*Prompt Communications*

In all matters relevant to customers, suppliers, government authorities, the public and others in the Organization, all employees must make every effort to achieve complete, accurate, and timely communications—responding promptly and courteously to all proper requests for information and to all complaints.

*Privacy and Confidentiality*

When handling financial and personal information about customers or others with whom the Organization has dealings, observe the following principles:

1. Collect, use, and retain only the personal information necessary for the Organization's business. Whenever possible, obtain any relevant information directly from the person concerned. Use only reputable and reliable sources to supplement this information.
2. Retain information only for as long as necessary or as required by law. Protect the physical security of this information.
3. Limit internal access to personal information to those with a legitimate business reason for seeking that information. Use only personal information for the purposes for which it was originally obtained. Obtain the consent of the person concerned before externally disclosing any personal information, unless legal process or contractual obligation provides otherwise.